

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

Mathew Harley , et al.,

Plaintiffs,

- against -

Peter S. Kosinski, et al.,

Defendants.

Case No: 20-CV-4664

**DECLARATION OF
SUSAN GREENHALGH**

SUSAN GREENHALGH declares the following to be true and correct under penalty of perjury, pursuant to 28 U.S.C. § 1746:

1. I am the senior advisor for election security to Free Speech For People, a non-partisan, not for profit 501c3 organization committed to protecting democracy for all the people.
2. I am of legal age and competent to provide this affidavit. All the information herein is based on my own personal knowledge unless otherwise indicated.
3. I have studied and worked in the area of election security and election technology for over 15 years.
4. I have researched policies, procedures and laws regarding the electronic return of voted ballots extensively from 2007 to the present. I have been invited to speak on internet voting at the International Association of Government Officials, the Mid-West Election Officials' conferences and at multiple conferences for the Election Verification Network. I have been invited to brief congressional staffers in both the U. S. House and Senate on internet voting.

5. In 2018, I was the primary author of the report “Email and Internet Voting: The Overlooked Threat to Election Security,” which was co-authored by Jeremy Epstein of the Association for Computing Machinery, U.S. Technology Policy Committee, Paul Rosenzweig of the R Street Institute and Susannah Goodman of the Common Cause Education Fund.¹ I presented this paper to the State Election Officials’ Testing and Certification Conference in 2019.
6. In 2020, I was the primary author of the white paper “Leveraging Electronic Balloting Options Safely and Securely During the COVID-19 Pandemic,”² with Dr. Steve Newell of the American Association for the Advancement of Sciences’ Center for Evidence in Public Issues. We presented this paper at the State Election Officials’ Testing and Certification Conference and the DEF CON computer security conference this summer.
7. I submit this Declaration in opposition to the plaintiffs’ motion for a preliminary injunction that would require election officials of seven states to “accept voted ballots from overseas voters that are sent via email or facsimile to the local election office (whether directly or through DoD Fax).”
8. Plaintiffs’ complaint suffers from several erroneous conclusions and assumptions derived from a lack of historical and factual context regarding internet voting in the United States.

Congressional record on internet voting

9. In effect, plaintiffs are asking this Court to do what Congress has refused to pursue or require.

¹ Available at: <https://www.acm.org/binaries/content/assets/public-policy/jtreportemailinternetvoting.pdf>

² Available at: https://freespeechforpeople.org/wp-content/uploads/2020/06/rabm.white_paper_6.23.20.pdf

10. Plaintiffs' complaint is based on the flawed assumption that voted ballots can be returned securely and reliably, and suggests that by dedicating sufficient government resources to this problem it could be solved easily. But Plaintiffs' complaint appears ignorant of over two decades of research and over a \$100 million spent by federal and state governments in search of secure online ballot return methods, and the federal government's ultimate decision to abandon an effort to develop an online voting system for military and overseas voters because of overwhelming evidence that it could not be done securely.
11. In 2002, in the National Defense Authorization Act (NDAA) Congress directed the Department of Defense (DOD), through its agency the Federal Voting Assistance Program (FVAP), to develop an online ballot return system for military and overseas voters.³
12. A system was developed at the direction of the FVAP, termed the Secure Electronic Voting and Registration Experiment (SERVE), aimed to be deployed in the 2004 general elections.
13. At the request of the DOD, security researchers examined the security of the SERVE system and found that it could not reliably secure ballots cast over the internet. Researchers concluded that the insurmountable challenge to securing an online voting system lies in the fundamentally insecure nature of the internet, writing:

"We do not believe that a differently constituted project could do any better job than the current team. The real barrier to success is not a lack of vision, skill, resources, or dedication; it is the fact that, given the current Internet and PC security technology, the FVAP has taken on an

³ Public Law 107-107 National Defense Authorization Act 2002. 115 Stat 1052

essentially impossible task.”⁴

14. In January of 2004, Deputy Secretary of Defense Paul Wolfowitz cancelled the project based on the conclusion that the system could not ensure the legitimacy of ballots cast over the internet.⁵
15. In response, in 2005 Congress amended its directive in the NDAA and tasked the U.S. Election Assistance Commission (EAC) and the National Institute of Standards and Technology (NIST) to study online and email ballot return in order to develop a set of standards for a secure, remote electronic absentee voting system that could be applied to secure the next system developed by the FVAP to replace SERVE.⁶
16. NIST analyzed the security challenges associated with remote electronic voting in several reports and identified multiple obstacles to reliably authenticating voters’ identities and transmitting ballots securely that have not yet been overcome. In 2011, NIST issued a summary of its research and findings that concluded that secure, electronic, voted ballot transmission was not yet feasible, writing:

*“Internet voting systems cannot currently be audited with a comparable level of confidence in the audit results as those for polling place systems. Malware on voters’ personal computers poses a serious threat that could compromise the secrecy or integrity of voters’ ballots. And, the United States currently lacks a public infrastructure for secure electronic voter authentication. Therefore, NIST’s research results indicate that additional research and development is needed to overcome these challenges before secure Internet voting will be feasible.”*⁷
17. Additional research by state governments and private sector researchers agreed

⁴ Drs. David Jefferson, Aviel D. Rubin, Barbara Simons, and David Wagner, “A Security Analysis of the Secure Electronic Registration and Voting Experiment (SERVE), Jan. 5, 2004. Available at: <http://euro.ecom.cmu.edu/program/courses/tcr17-803/MinorityPaper.pdf>

⁵ Jim Garamone, “Pentagon Decides Against Internet Voting This Year,” *Armed Forces Press Services* (February 6, 2004), <http://archive.defense.gov/news/newsarticle.aspx?id=27362>.

⁶ The Ronald W. Reagan Defense Authorization Act for FY2005 (P.L. 108-375)

⁷ See “NIST Activities on UOCAVA Voting,” *NIST Information Technology Laboratory* (August 25, 2016), <https://www.nist.gov/itl/voting/nist-activities-uocava-voting>.

with NIST's conclusions. In 2008, 32 respected computer scientists issued a statement opposing the adoption of online voting in public elections, warning that serious and potentially insurmountable challenges stood in the way of creating a safe internet-based voting system.⁸

18. In 2010, an online voting pilot in the District of Columbia was scheduled to be deployed for the November 2010 elections. Prior to going live, the system was available to the public and researchers that wished to try the system and test its security. Within 36 hours, researchers at the University of Michigan had completely compromised the system and were able to substitute fraudulent ballots for legitimate ones. The breach was undetected by the DC election officials.⁹

19. The Utah Lt. Governor convened an iVote Advisory Committee to explore online voting. In its final report delivered in August of 2015, the Committee wrote:

*"Given that sufficiently secure Internet voting systems do not yet exist, they would need to be built. Of course, some systems, like a stone bridge to the moon, are impossible to build. Others, like a stone bridge to Hawaii, are so exorbitantly expensive as to remain a fool's errand. However, other systems, like spacecraft, aircraft, and the newer Sam White Bridge, are much more affordable. Unfortunately, with the four challenges mentioned in the preceding section, the unconstrained nirvana of Internet voting, "from any device, entirely online," is so impossible, or at least infeasible, as to be a fool's errand."*¹⁰

20. With evidence mounting that a secure online voting system was not possible, and NIST's conclusion that it could not develop standards capable of securing an online voting system for military and overseas voters, Congress abandoned the

⁸ "Computer Technologists' Statement on Internet Voting," *Verified Voting* (2008), <http://www.verifiedvoting.org/wp-content/uploads/2012/09/InternetVotingStatement.pdf>.

⁹ Sarah Wheaton, "Voting Test Falls Victim to Hackers," *The New York Times*, (Oct. 8, 2010). Available at: <https://www.nytimes.com/2010/10/09/us/politics/09vote.html>

¹⁰ iVote Advisory Committee Final Report, Utah Lt. Governor, Spencer J. Cox, (Aug. 21, 2015). Available at: <https://elections.utah.gov/Media/Default/Documents/Report/iVote%20Report%20Final.pdf>

development of an online voting system and repealed its directive to FVAP to develop a remote electronic voting system in the 2015 NDAA.¹¹

21. Separately, in 2010, Congress passed the Military and Overseas Voter Empowerment (MOVE) Act to improve access to the ballot for military and overseas voters established in the Uniform and Overseas Citizens' Absentee Voting Act (UOCAVA). In an effort to facilitate voting for UOCAVA voters, the MOVE Act required states to adopt systems and procedures to allow UOCAVA voters to register to vote online, to request an absentee ballot online, and to receive a *blank* absentee ballot electronically, via email or an online portal.¹²
22. While the MOVE Act provided for the possibility of pilot programs for the electronic return of voted ballots, Congress notably did not appropriate funding for such pilot programs under MOVE, and these pilots were never brought to fruition. Instead, Congress provided funding to FVAP to offer Electronic Absentee Systems for Elections (EASE) grants to states to support the other provisions in the MOVE Act. The grant terms and contracts explicitly prohibited states from using the money for the electronic return of voted ballots in live elections."¹³
23. Congress extended the EASE grant program in 2013, again specifically prohibiting the use of EASE 2 grant funds for the electronic return of voted ballots.¹⁴

¹¹ "Voting Demonstration Project Repealed," *U.S. Vote Foundation*, <https://www.usvotefoundation.org/blog/domestic-voting/voting-demonstration-project-repealed>.

¹² Available at: <https://www.congress.gov/bill/111th-congress/senate-bill/1415/text>

¹³ Electronic Absentee Systems for Elections (EASE) Grants For States, Territories and Localities Broad Agency Announcement H98210-BAA-11-0001 Available at: https://www.fvap.gov/uploads/FVAP/Grants/EASE_BAA.pdf

¹⁴ "DoD ANNOUNCES GRANTS PROGRAM TO EASE VOTING PROCESS Funding Available for Research

24. The historical record shows clearly that Congress has deliberately contemplated and engaged on the issue of remote electronic voting for military and overseas voters and has determined that it cannot be done securely and should not be funded or promoted by the federal government. Plaintiffs are asking the Court to ignore the science and take action that Congress has plainly determined is ill-advised.

Though states permit online voting, this does not mean it's secure

25. Though Congress has wisely declined to require or fund online voting for military and overseas voters, over thirty states have adopted this unwise practice. Plaintiffs draw the erroneous conclusion that this means it is safe and reliable.
26. When considering why so many states currently permit online voting, it is important to take into account historical context. Most of the states that currently permit electronic ballot return adopted these policies in the late 20th century or the first decade of the 2000s. During this period, as described above, there was an expectation that the FVAP and the DOD would develop and offer an online voting system. States passed laws to permit online ballot return with the expectation that a secure online voting system from the DOD would be available in the near term.
27. In addition, the risks of hacking were not as commonplace as they are today, and cybercrime and identity theft were much less mature. Thus, there was less awareness of the prospect of online attacks. Furthermore, the U.S. had not yet

learned that foreign adversaries were actively trying to compromise our election infrastructure. We cannot ignore these facts today.

28. In fact, in an effort to reverse this risky policy in Washington State, the Secretary of State supported legislation last session to remove the provision to allow military and overseas voters to return ballots over the internet citing the increased security threats facing our nation's elections.¹⁵

Plaintiffs overlook constitutional requirements for a secret ballot

29. Plaintiffs glancingly acknowledge that email and fax return of voted ballots cannot preserve ballot secrecy and protect voter's right to cast a private ballot, but they carelessly ignore the fact that all seven defendant states have constitutional provisions that guarantee secrecy in voting.¹⁶

Plaintiffs ignore DOD's policy to limit its fax service

30. In the requested relief, Plaintiffs suggest that voters can easily use the DOD's fax service but Plaintiffs do not acknowledge that the DOD explicitly took actions to limit the use of this service in January 2018 because of extremely high volume of submissions.¹⁷ Returning ballots via the DOD's email to fax program includes the same serious and insoluble security vulnerabilities identified by computer security

¹⁵ HB 2111 <http://lawfilesexternal.wa.gov/biennium/2019-20/Pdf/Bill%20Reports/House/2111%20HBA%20SGOV%2020.pdf?q=20201008160117>

¹⁶ Caitriona Fitzgerald, Pam Smith, Susannah Goodman, "*The Secret Ballot at Risk, Recommendations for Protecting Democracy*," Electronic Privacy Information Center, Verified Voting, Common Cause, Aug. 28, 2018. Available at: <https://epic.org/2016/08/epic-verified-voting-common-ca.html>

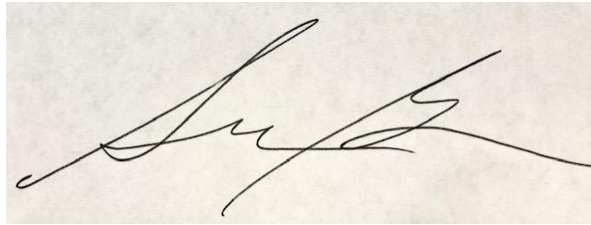
¹⁷ See: <https://www.fvap.gov/info/news/2017/9/19/message-from-the-fvap-director-upcoming-changes-to-ets>

experts in study after study. Overburdening the DOD's system further would only weaken an already insecure and unreliable process.

I affirm, under the penalties for perjury, that the foregoing representations are true and accurate to the best of my knowledge.

Dated: October 8, 2020

[Amityville, NY]

A handwritten signature in black ink on a light-colored, textured background. The signature is cursive and stylized, appearing to read 'Susan Greenhalgh'.

Susan Greenhalgh